МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АЛГОРИТМЫ ШИФРОВАНИЯ ИНФОРМАЦИИ

наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: ст.преподаватель кафедры ИиИБ, к. т.н.
(должность, ученая степень, ученое звание)

_____ / М.В. Коновалов /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики и информационных технологий, к.п.н., профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина /
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1.Цели освоения дисциплины

Целями освоения дисциплины «Алгоритмы шифрования информации» является формирование у обучающихся понятий об основных методах шифрования, криптографических протоколах, базовых алгоритмах, применяемых в криптосистемах, алгоритмах шифрования с симметричным и несимметричным ключом. Овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2.Место дисциплины в структуре образовательной программы специалиста

Дисциплина «Алгоритмы шифрования» входит в вариативную часть блока №1 образовательной программы.

Для усвоения данной дисциплины обучающемуся необходим объём знаний, предусмотренный курсами информатики, дискретной математики, организации ЭВМ и вычислительных систем, технологии и методы программирования, языки программирования.

Данная дисциплина необходима для последующего успешного выполнения научно-исследовательской работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

Структурный элемент компетенции	Планируемые результаты обучения
ПК-9. Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать:	Классификацию методов шифрования сообщений. Основы теории засекреченной связи. Математические операции, применяемые при шифровании данных.
Уметь:	Применять алгоритмы блочного шифрования при разработке ПО. Применять алгоритмы симметричного шифрования при разработке ПО
Владеть:	Навыками частотного анализа; Навыками применения метода полного перебора; Навыками атаки на закрытое и открытое сообщение.
ПК-10. способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать:	Системы блочного шифрования. Системы симметричного шифрования Хеш-функции; Протоколы обмена ключами.
Уметь:	Реализовывать на языках высокого уровня алгоритмы шифров однозначной замены; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров; Реализовывать на языках высокого уровня алгоритмы омофонических шифров; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров.
Владеть	Навыками разработки защищенного программного обеспечения с

Структурный элемент компетенции	Планируемые результаты обучения
:	применением шифров гаммирования; Навыками разработки защищенного программного обеспечения с применением комбинированных шифров; Навыками разработки защищенного программного обеспечения с применением шифров с открытым ключом;

4.Структура и содержание дисциплины «Алгоритмы шифрования информации»

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 часов, в том числе:

– контактная работа – 87,8 акад. часов:

– аудиторная – 85 акад. часов;

– внеаудиторная – 2,8 акад. часов;

–самостоятельная работа – 92,2 акад. часов;

– вид аттестации – зачет с оценкой.

Раздел дисциплины	Сем.	Аудиторная контактная работа		Самостоятельная работа	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	практика				
Модуль 1. Введение в шифрование							
Шифры замены и перестановки. Типы атак на примитивные шифры.	8	2	7/4И	13	Подбор, описание, экспертная оценка сайтов Интернет, разработка глоссария к теме.	семинарское занятие, контрольная работа	ПК-9 зув ПК-10 зув
Модуль 2. Симметричные криптографические системы							
Блочные шифры. Составные шифры. Атаки на блочные шифры.	8	2	7/3И	13	Выполнение индивидуального домашнего задания	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9 зув ПК-10 зув
Модуль 3. Потоковые шифры и генераторы ГСПЧ							
Общие сведения. Принципы использования ГСПЧ. Классификация потоковых шифров. Шифр A5. Шифр RC4.	8	2	7/3И	13	Выполнение индивидуального домашнего задания	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9 зув ПК-10 зув
Модуль 4. Блочное симметричное шифрование данных (DES)							
Принципы построения алгоритма DES. Анализ алгоритма DES. Безопасность DES.	8	7	8/3И	13	Выполнение индивидуального домашнего задания	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9 зув ПК-10 зув
Модуль 5. ГОСТ 28147-89.							
Математический базис ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Безопасность ГОСТ 28147-89.	8	7	8/3И	13	Выполнение индивидуального домашнего задания	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9 зув ПК-10 зув
Модуль 6. AES.							
Математический базис AES. Формат данных AES. Структура алгоритма и раундов AES. Стойкость AES.	8	7	7/3И	14,2	Выполнение индивидуального домашнего задания	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9 зув ПК-10 зув
Модуль 7. IDEA							
Структура алгоритма IDEA. Шифрование данных IDEA. Безопасность IDEA.	8	7	7	13			
Итого по курсу:		34	51/22И	92,2	Зачет с оценкой		ПК-9 зув ПК-10 зув

И – часы в интерактивной форме, ИДЗ – индивидуальное домашнее задание.

5. Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Алгоритмы шифрования информации» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

- обзорные лекции – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;
- лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;
- Семинар.
- Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

проблемная - для развития исследовательских навыков и изучения способов решения задач.

лекции с заранее запланированными ошибками – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения

Творческий проект – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

Формы учебных занятий с использованием информационно-коммуникационных технологий:

- Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
- Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.
- методы IT
  - Подготовка и проведение лабораторных работ по поиску информации в сетях. Задание критериев поиска информации. Работа с поисковыми системами университета и внешними ресурсами.
  - Подготовка и проведение лабораторных работ по Архивации данных с целью дальнейшего использования в средствах телекоммуникационных технологий: электронной почте, чате, телеконференции т.д.
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий (платформа e-Learning).
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
  - Компьютерный практикум.
- работа в команде
  - Разработка Web-проектов.
- case-study
  - Разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
- проблемное обучение
  - Подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.
- учебная дискуссия
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- использование тренингов
  - Подготовка и проведение демонстрационных, тематических и итоговых

компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Алгоритмы шифрования информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерный индивидуальные домашние задания

Модуль 1. Введение в шифрование.

1. Дан шифротекст «ШДЁЮЧЖЪХЩЖАЮВЕБХВЪГЪВ». Необходимо получить открытое сообщение.

2. Дан шифротекст и открытый текст. Определить ключ, если известно что использован шифр Виженера.

Шифротекст

ЮУТПЕФОЪХЯНФЭЕЭЧАЛТВЯХНРЩТМЯЪКЛСТЦРЙТСЫАЬЫКУЭЦОРЩШЙНЧ
ХОФЦТЙЭЫЖЦЯЫРЧРЮЖЫЗМГРУЙПЙЫЦЦМТШЕЮЯОЧЦРЩРТЬЮЙНСЯЫТ
ЦФДФГЯАЬАВЫНЩЦРЫОБОИДЕЪОУКХЪВТМЬЧАУНЖЬДХЧНЯАСЩШЕФЦТЙ
ЕМНЮТТЛРЩЫСЮЧНМУОЗНОУИГЬЧСЕБТЙУДУЭСЩУККЯМЕГНМЭЕЦЧПЫЖЬ
БЫЕГЩИЦЗШНМАЩФОЬДЪЦУШОЫТЧЖСВЩИЪБЫБЯПВКНЦЪЧХТОУЬЪЛУЗ
ЗЦЕЮКЖЭПСЙКВЯТЖЪАПРЦЮТХЕМЕОТТМШПНЪЪЕВЩДШЧЮПДУЮУПКР
ИСШГЫБПЗЙЖЦХСГЧСЕТТЕЖЗУРВФНВАСЕЩШЖЮГРРГЫБМДЫКСКРИЭЪЯ
РОЫАФАЮЮПНВПТСЫАРУФРФТЪАЬСУОТЛХКЧФВИЦСВТЧЙИУЗНОЖЮБНЯЬ
ЕЬЗРФЪЭАЩГВЫЕДУЗШНУЬТТЯМГСУДТДХКЦЕГРИХЩЛЭУУОУЬБШНЕУМТД

Открытый текст

Неспокойные времена настали для Галактической Республики Налогообложение торговых путей к отдаленным солнечным системам стало причиной раздоров В стремлении добиться своего обуянная алчностью Торговая Федерация с помощью мощных боевых кораблей взяла в кольцо блокады маленькую планету Набу лишив её всех поставок В то время как члены Конгресса Республики ведут напряженные дебаты в связи с тревожными событиями Верховный канцлер втайне от всех поручил двум рыцарям джедай хранителям мира и справедливости в Галактике урегулировать конфликт

Модуль 2. Симметричные криптографические системы

1. Укажите различия между современными и традиционными шифрами с симметричным ключом.

2. Объясните, почему современные блочные шифры спроектированы как шифры подстановки вместо того, чтобы применять шифры транспозиции.

3. Перечислите компоненты современного блочного шифра.

4. Определите *P*-блок и назовите его три варианта. Какой вариант является обратным?

5. Сообщение имеет 1500 символов для представления, которых используются *ASCII* коды. Это сообщение будет зашифровано блочным шифром длиной *64* бита. Найдите размер дополнения и количество зашифрованных блоков.

6. Покажите Р-блок, определен последовательностью: 81234567.

Модуль 3. Потоковые шифры и генераторы ГСПЧ

1. Определите последовательность из первых десяти чисел и период линейного конгруэнтного *ГПСЧ* для *a=5*, *b=7* и *c=17* (*k_0* принять равным – *0*).

2. Определите последовательность из десяти чисел, генерируемой методом Фибоначчи с задержкой, начиная с k_a при a = 3, b = 1, k_0 =0,6, k_1 =0,3, k_2 =0,5.

3. Вычислить псевдослучайную двоичную последовательность длиной 12 бит по методу генерации ПСЧ BBS, если: p = 19, q = 23, x = 3.

Модуль 4. Блочное симметричное шифрование данных (DES)

1. Значение последовательности входных данных в DES равно: $1234567890ABCDEF_{16}$. Определить значение последовательности на выходе блока IP-перестановки.

2. Значение последовательности R_0 в DES равно: $R_0 = F0AAE8A5_{16}$. Определить значение последовательности на выходе *E*-блока перестановки и расширения.

3. Значение последовательности R_1 в DES равно: $R_1 = 116BA133_{16}$. Определить значение последовательности на выходе *E*-блока перестановки и расширения.

Модуль 5. ГОСТ 28147-89

1. В регистре N_1 алгоритма ГОСТ 28147-89 находятся данные:N_1 – $191A2AB8_{16}$, в N_2 – $434665B2_{16}$. Ключ для шифрования $k_0=EB8A7159_{16}$, $k_2=7CE5D63D_{16}$, $k_3=4AC1D6E0_{16}$, $k_4=BAFE4731_{16}$, $k_5=A3DEB025_{16}$, $k_6=8BB389AC_{16}$, $k_7=10D3B61A_{16}$, $k_8=E9AC340F_{16}$. Цикл шифрования – 25. Что будет находится в N_1 и N_2 после завершения цикла. Использовать структуру режима простой замены.

Модуль 6. AES

1. Произвести сложение двух элементов конечного поля $x_7 + x_3 + x + 1$ и $x_6 + x_3 + x_2 + 1$.

2. Определить аддитивную инверсию многочлена длиной в один байт из конечного поля *GF(2^8)* x6+x3+x2+1.

3. Значения байтов матрицы состояния данных на входе функции SubBytes() AES-128 равны $A49C7FF2689F352B6B5BEA43026A5049_{16}$. Определить значения байтов матрицы состояния данных на выходе функции SubBytes().

Модуль 7. IDEA

1. Начальный ключ алгоритма IDEA – последовательность длиной 128 битов, которая равна K = $3F424CDC105CA00D7B3DBE8C96A2978E_{16}$. Сформировать раундовые ключи для второго раунда шифрования.

2. Определить результат этапа перестановки (трансформации) первого раунда шифрования алгоритмом *IDEA*, если входные данные равны: M = $3D550F51D71EE0AA_{16}$. Раундовые ключи шифрования: $k_1=3F42_{16}$, $k_2=4CDC_{16}$, $k_3=105C_{16}$, $k_4=A00D_{16}$.

Курсовая работа выполняется обучающимся самостоятельно под руководство преподавателя. При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В начале изучения дисциплины преподаватель предлагает обучающимся на выбор перечень тем курсовых работ. Обучающийся самостоятельно выбирает тему курсовой работы. Совпадение тем курсовых работ у обучающихся одной учебной группы не допускается. Утверждение тем курсовых работ проводится ежегодно на заседании кафедры.

После выбора темы преподаватель формулирует задание по курсовой работе и рекомендует перечень литературы для ее выполнения. Исключительно важным является использование информационных источников, а именно системы «Интернет», что даст возможность обучающимся более полно изложить материал по выбранной им теме.

В процессе написания курсовой работы обучающийся должен разобраться в

теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Преподаватель, проверив работу, может возвратить ее для доработки вместе с письменными замечаниями. Обучающийся должен устранить полученные замечания в установленный срок, после чего работа окончательно оценивается.

Курсовая работа должна быть оформлена в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления».

Примерный перечень тем курсовых работ и пример задания представлены в разделе «Оценочные средства для проведения промежуточной аттестации».

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-9. Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	Классификацию методов шифрования сообщений. Основы теории засекреченной связи. Математические операции, применяемые при шифровании данных.	1.Сформулируйте необходимое и достаточное условия для совершенной секретности криптографической системы. 2. Дайте объяснение сущности рассеивания данных в процессе их шифрования. 3. Что является целью перемешивания данных в процессе их шифрования? 4. Что такое криптографическая атака? 5. Какие типы криптографических атак существуют? 6. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность атаки “грубой силы”. 7. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность статистической атаки. 8. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность атаки по образцу. 9. Дайте характеристику атаки на известный входной текст. 10. Дайте характеристику атаки на выбранный входной текст. 11. Дайте характеристику атаки на выбранный зашифрованный текст.

Уметь	Применять алгоритмы блочного шифрования при разработке ПО. Применять алгоритмы симметричного шифрования при разработке ПО	1. *S*-блок подстановки производит операцию xor с нечетными битами, чтобы получить левый бит выхода, и xor с четными битами, чтобы получить правый бит выхода. Определить значение на выходе блока если на входе блока 110010_2 2. Крайний левый бит *S*-блока подстановки размером 4x3определяет смещение других трех бит. Если крайний левый бит равен 0, то три других бита перемещаются вправо на один бит. Если крайний левый бит равен 1, то три других бита перемещаются влево на один бит. Определить результат на выходе блока если на входе последовательность 1011_2.
Владеть	Навыками частотного анализа; Навыками применения метода полного перебора; Навыками атаки на закрытое и открытое сообщение.	1. Файл содержит сообщение зашифрованное шифром перестановки. Дешифровать сообщение при помощи метода полного перебора, и опираясь на статистические свойства сообщения. 2. Файл содержит открытое и закрытое сообщение, зашифрованное при помощи шифра перестановки. Определить ключ, используемый при шифровании.
ПК-10. способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	Комбинированное шифрование; Шифрование с открытым ключом; Хеш-функции; Протоколы обмена ключами.	1.Схема режима шифрования DES-ECB. 2. Схема режима шифрования DES-CBC. 3. Схема режима шифрования DES-CPB и DES-OFB. 4. Тройной DES. Сферы применения различных режимов DES. 5. Схема режима шифрования простой замены ГОСТ 28147-89. 6. Шифрование с открытым ключом. Основные понятия. 7. Алгоритм шифрования на основе эллиптических кривых.

Уметь	Реализовывать на языках высокого уровня алгоритмы шифров однозначной замены; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров;	Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи полибианского квадрата. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифрующей системы Тримесуса. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи биграммного шифра Порты. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра Хилла. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра Виженера. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи совмещенного шифра. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра маршрутной перестановки. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра «Перекресток». Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи решетки Кардано. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра RC4. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра ADFGX

Владеть	Навыками разработки защищенного программного обеспечения с применением шифров гаммирования; Навыками разработки защищенного программного обеспечения с применением комбинированных шифров; Навыками разработки защищенного программного обеспечения с применением шифров с открытым ключом;	1.Реализовать на языке C# программное средство осуществляющее шифрование изображения представленного в формате BMP при помощи Вернама. 2. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-ECB. 3. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-CBC. 4. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-CPB. 5. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-OFB. 5. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму тройной DES.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета и экзамена.

Показатели и критерии оценивания зачета с оценкой:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

«не зачтено» – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания курсовой работы:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения

информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

8.Учебно-методическое и информационное обеспечение дисциплины(модуля)

Основная литература

1. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. Режим доступа: http://znanium.com/bookread.php?book=441493. –Заглавие с экрана.– ISBN 978-5-7638-2113-7.
2. Программно-аппаратная защита информации [Электронный ресурс]: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.- (Высшее образование). . - Режим доступа: http://znanium.com/bookread.php?book=503511. –З аглавие с экрана. – ISBN 978-5-00091-004-7.

Дополнительная литература:

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.com.–Заглавие с экрана.
4. Баранкова И. И. Теория информации. Кодирование [Электронный ресурс] : учебное пособие / И. И. Баранкова, М. В. Коновалов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3313.pdf&show=dcatalogues/1/1137756/3313.pdf&view=true. - Макрообъект. - ISBN 978-5-9967-1073-7..

Интернет – ресурсы

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". URL: http://www.osp.ru/os/– Загл. с экрана. Яз. рус.
5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.
6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.
7. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные : периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
8. http://www.безопасник.рф

9. Материально-техническое обеспечение дисциплины(модуля)

Тип и название аудитории	Оснащение аудитории
Лекционная аудитории 282, 374, 388	Мультимедийные средства хранения, передачи и представления информации
Компьютерные классы 372-1-5	Персональные компьютеры под управление ОС Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) с пакетом MS Office 2007 (Microsoft Open License 42649837), выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Аудитории для самостоятельной работы: компьютерные классы 132; читальные залы, библиотеки.	Персональные компьютеры под управление ОС Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) с пакетом MS Office 2007 (Microsoft Open License 42649837), выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем». Специализация «Обеспечение информационной безопасности распределенных информационных систем».